The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
advanced_links_management -- advanced_links_management	SQL injection vulnerability in read.php in Advanced Links Management (ALM) 1.5.2 allows remote attackers to execute arbitrary SQL commands via the catId parameter.	unknown 2008-06-03	7.5	CVE-2008-2529 MILW0RM BID XF
AJ Square -- AJ HYIP	SQL injection vulnerability in forum/topic_detail.php in AJ Square aj-hyip (aka AJ HYIP Acme) allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-06-03	7.5	CVE-2008-2532 MILW0RM BID
Akamai Technologies -- Download Manager	Unspecified vulnerability in Akamai Download Manager ActiveX control before 2.2.3.6 allows remote attackers to force the download and execution of arbitrary files via unknown vectors.	unknown 2008-06-04	9.3	CVE-2008-1770 BUGTRAQ
Apple -- Mac OS X Server Apple -- Mac OS X	Unspecified vulnerability in AppKit in Apple Mac OS X before 10.5 allowsuser-assisted remote attackers to execute arbitrary code or cause a denial ofservice (application crash) via a crafted document file, as demonstrated byopening the document with TextEdit.	unknown 2008-06-02	7.5	CVE-2008-1028 APPLE CERT BID SECTRACK XF
Apple -- Mac OS X Server Apple -- Mac OS X	Integer overflow in the CFDataReplaceBytes function in the CFData API inCoreFoundation in Apple Mac OS X before 10.5.3 allows context-dependentattackers to execute arbitrary code or cause a denial of service (crash) via aninvalid length argument, which triggers a heap-based buffer overflow.	unknown 2008-06-02	7.5	CVE-2008-1030 APPLE CERT BID SECTRACK XF
Apple -- Mac OS X Server Apple -- Mac OS X	Integer overflow in ImageIO in Apple Mac OS X before 10.5.3 allows remoteattackers to execute	unknown 2008-06-02	9.3	CVE-2008-1574 BID

	arbitrary code or cause a denial of service (applicationcrash) via a crafted JPEG2000 image that triggers a heap-based bufferoverflow.			SECTRACK XF
Apple -- Mac OS X Server Apple -- Mac OS X	Unspecified vulnerability in the Apple Type Services (ATS) server in AppleMac OS X 10.5 before 10.5.3 allows user-assisted remote attackers to executearbitrary code via a crafted embedded font in a PDF document, related to memorycorruption that occurs during printing.	unknown 2008-06-02	9.3	CVE-2008-1575 BID SECTRACK XF
Apple -- Mac OS X Server Apple -- Mac OS X	Mail in Apple Mac OS X before 10.5, when an IPv6 SMTP server is used, doesnot properly initialize memory, which might allow remote attackers to executearbitrary code or cause a denial of service (application crash), or obtainsensitive information (memory contents) in opportunistic circumstances, bysending an e-mail message.	unknown 2008-06-02	7.5	CVE-2008-1576 APPLE CERT BID XF
Apple -- Mac OS X Server Apple -- Mac OS X	Unspecified vulnerability in the Pixlet codec in Apple Pixlet Video inApple Mac OS X before 10.5.3 allows remote attackers to execute arbitrary codeor cause a denial of service (application crash) via a crafted movie file,related to "multiple memory corruption issues."	unknown 2008-06-02	9.3	CVE-2008-1577 BID SECTRACK XF
Apple -- Safari	Apple Safari does not prompt the user before downloading an object that has an unrecognized content type, which allows remote attackers to place malware into the (1) Desktop directory on Windows or (2) Downloads directory on Mac OS X, aka a "Carpet Bomb," a different issue than CVE-2008-1032. NOTE: Apple reportedly has stated that "we are not treating this as a security issue." NOTE: Microsoft describes the issue on the Windows platform as "a blended threat that allows remote code execution."	unknown 2008-06-03	9.3	CVE-2008-2540 OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID SECTRACK XF
Battle.net Clan Script -- Battle.net Clan Script	SQL injection vulnerability in members.php in Battle.net Clan Script for PHP 1.5.3 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the showmember parameter in a members action.	unknown 2008-06-03	7.5	CVE-2008-2522 MILW0RM BID
BigACE -- BigACE	Multiple PHP remote file inclusion vulnerabilities in BigACE 2.4, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) GLOBALS[_BIGACE][DIR][addon] parameter to (a) addon/smarty/plugins/function.captcha.php and (b) system/classes/sql/AdoDBConnection.php; and the (2) GLOBALS[_BIGACE][DIR][admin] parameter to (c) item_information.php and (d) jstree.php in system/application/util/, and (e) system/admin/plugins/menu/menuTree/plugin.php, different vectors than CVE-2006-4423.	unknown 2008-06-03	7.5	CVE-2008-2520 MILW0RM
BP Blog -- BP Blog	Multiple SQL injection vulnerabilities in BP Blog 6.0 allow remote attackers to execute arbitrary	unknown 2008-06-05	7.5	CVE-2008-2554 BUGTRAQ

	SQL commands via the (1) id parameter to template_permalink.asp and (2) cat parameter to template_archives_cat.asp.			MILW0RM BID
CA -- Internet Security Suite Plus 2008	Directory traversal vulnerability in the UmxEventCli.CachedAuditDataList.1(aka UmxEventCliLib) ActiveX control in UmxEventCli.dll in CA Internet SecuritySuite 2008 allows remote attackers to create and overwrite arbitrary files via a. (dot dot) in the argument to the SaveToFile method. NOTE: this can beleveraged for code execution by writing to a Startup folder. NOTE: some ofthese details are obtained from third party information.	unknown 2008-06-02	9.3	CVE-2008-2511 BUGTRAQ MILW0RM OTHER-REF SECTRACK
CA -- etrust_secure_content_manager	Multiple stack-based buffer overflows in the HTTP Gateway Service in CA eTrust Secure Content Manager 8.0 allow remote attackers to execute arbitrary code or cause a denial of service via crafted FTP requests, related to (1) the file month field in a LIST command; (2) the PASV command; and (3) directories, files, and links in a LIST command.	unknown 2008-06-04	10.0	CVE-2008-2541 OTHER-REF
Cisco -- Adaptive Security Appliance Cisco -- pix_security_appliance	Cisco Adaptive Security Appliance (ASA) and Cisco PIX security appliance 7.1.x before 7.1(2)70 and 8.0.x before 8.0(3)10 allows remote attackers to cause a denial of service via a crafted TCP ACK packet to the device interface.	unknown 2008-06-04	7.8	CVE-2008-2055 SECTRACK
Cisco -- Adaptive Security Appliance Cisco -- pix_security_appliance	Cisco Adaptive Security Appliance (ASA) and Cisco PIX security appliance 8.0.x before 8.0(3)9 and 8.1.x before 8.1(1)1 allows remote attackers to cause a denial of service (device reload) via a crafted Transport Layer Security (TLS) packet to the device interface.	unknown 2008-06-04	7.8	CVE-2008-2056 SECTRACK SECTRACK
Cisco -- Adaptive Security Appliance Cisco -- pix_security_appliance	Cisco Adaptive Security Appliance (ASA) and Cisco PIX security appliance 7.2.x before 7.2(3)2 and 8.0.x before 8.0(2)17 allows remote attackers to cause a denial of service (device reload) via a port scan against TCP port 443 on the device.	unknown 2008-06-04	7.8	CVE-2008-2058 SECTRACK SECTRACK
Cisco -- Adaptive Security Appliance Cisco -- pix_security_appliance	Cisco Adaptive Security Appliance (ASA) and Cisco PIX security appliance 8.0.x before 8.0(3)9 allows remote attackers to bypass control-plane ACLs for the device via unknown vectors.	unknown 2008-06-04	7.8	CVE-2008-2059 CISCO SECTRACK SECTRACK
Citrix -- Access Gateway	Unspecified vulnerability in Citrix Access Gateway Standard Edition 4.5.7 and earlier and Advanced Edition 4.5 HF2 and earlier allows attackers to bypass authentication and gain "access to network resources" via unspecified vectors.	unknown 2008-06-03	10.0	CVE-2008-2528 FRSIRT
CMS -- EasyWay	SQL injection vulnerability in index.php in EasyWay CMS allows remote attackers to execute arbitrary SQL commands via the mid parameter.	unknown 2008-06-05	7.5	CVE-2008-2555 MILW0RM XF
damian_frizza -- Borland Interbase	Integer overflow in Borland Interbase 2007 SP2 (8.1.0.256) allows remote attackers to execute arbitrary code via a malformed packet to TCP port	unknown 2008-06-05	7.5	CVE-2008-2559 OTHER-REF BID

	3050, which triggers a stack-based buffer overflow. NOTE: this issue might be related to CVE-2008-0467.			SECTRACK
Fedora 8 -- consolehelper	The default configuration of consolehelper in system-config-network before1.5.10-1 on Fedora 8 lacks the USER=root directive, which allows local users ofthe workstation console to gain privileges and change the networkconfiguration.	unknown 2008-06-02	7.2	CVE-2008-2359 OTHER-REF FEDORA
fkrauthan -- phoenix_view_cms	Directory traversal vulnerability in admin/admin_frame.php in Phoenix View CMS Pre Alpha2 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the ltarget parameter.	unknown 2008-06-03	7.5	CVE-2008-2534 MILW0RM XF
fkrauthan -- phoenix_view_cms	Multiple SQL injection vulnerabilities in Phoenix View CMS Pre Alpha2 and earlier allow remote attackers to execute arbitrary SQL commands via the del parameter to (1) gbuch.admin.php, (2) links.admin.php, (3) menue.admin.php, (4) news.admin.php, and (5) todo.admin.php in admin/module/.	unknown 2008-06-03	7.5	CVE-2008-2535 MILW0RM XF
GNOME -- Evolution	Buffer overflow in Evolution 2.22.1, when the ITip Formatter plugin is disabled, allows remote attackers to execute arbitrary code via a long timezone string in an iCalendar attachment.	unknown 2008-06-04	7.6	CVE-2008-1108 OTHER-REF
GNOME -- Evolution	Heap-based buffer overflow in Evolution 2.22.1 allows user-assisted remote attackers to execute arbitrary code via a long DESCRIPTION property in an iCalendar attachment, which is not properly handled during a reply in the calendar view (aka the Calendars window).	unknown 2008-06-04	9.3	CVE-2008-1109
hessel_brouwer -- php_visit_counter	SQL injection vulnerability in read.php in PHP Visit Counter 0.4 and earlier allows remote attackers to execute arbitrary SQL commands via the datespan parameter in a read action.	unknown 2008-06-05	7.5	CVE-2008-2556 MILW0RM XF
HispaH -- Model Search	SQL injection vulnerability in cat.php in HispaH Model Search allows remote attackers to execute arbitrary SQL commands via the cat parameter.	unknown 2008-06-03	7.5	CVE-2008-2537 MILW0RM BID XF
HP -- Instant Support	Unspecified vulnerability in a certain ActiveX control in HPISDataManager.dll in HP Instant Support before 1.0.0.24 allows remote attackers to execute arbitrary code via unknown vectors, a different vulnerability than CVE-2007-5605, CVE-2007-5606, and CVE-2007-5607.	unknown 2008-06-04	7.5	CVE-2007-5604 HP
HP -- Instant Support	Unspecified vulnerability in a certain ActiveX control in HPISDataManager.dll in HP Instant Support before 1.0.0.24 allows remote attackers to execute arbitrary code via unknown vectors, a different vulnerability than CVE-2007-5604, CVE-2007-5606, and CVE-2007-5607.	unknown 2008-06-04	9.3	CVE-2007-5605 HP

HP -- Instant Support	Unspecified vulnerability in a certain ActiveX control in HPISDataManager.dll in HP Instant Support before 1.0.0.24 allows remote attackers to execute arbitrary code via unknown vectors, a different vulnerability than CVE-2007-5604, CVE-2007-5605, and CVE-2007-5607.	unknown 2008-06-04	10.0	CVE-2007-5606 HP
HP -- Instant Support	Unspecified vulnerability in a certain ActiveX control in HPISDataManager.dll in HP Instant Support before 1.0.0.24 allows remote attackers to execute arbitrary code via unknown vectors, a different vulnerability than CVE-2007-5604, CVE-2007-5605, and CVE-2007-5606.	unknown 2008-06-04	7.5	CVE-2007-5607 HP
HP -- Instant Support	Unspecified vulnerability in a certain ActiveX control in HPISDataManager.dll in HP Instant Support before 1.0.0.24 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-0952 and CVE-2008-0953.	unknown 2008-06-04	9.3	CVE-2007-5608
HP -- Instant Support	Unspecified vulnerability in a certain ActiveX control in HPISDataManager.dll in HP Instant Support before 1.0.0.24 allows remote attackers to cause a denial of service via unknown vectors.	unknown 2008-06-04	10.0	CVE-2007-5610 HP
HP -- Instant Support	Unspecified vulnerability in a certain ActiveX control in HPISDataManager.dll in HP Instant Support before 1.0.0.24 has unknown impact and remote attack vectors, a different vulnerability than CVE-2007-5608 and CVE-2008-0953.	unknown 2008-06-04	9.3	CVE-2008-0952 HP
HP -- Instant Support	Unspecified vulnerability in a certain ActiveX control in HPISDataManager.dll in HP Instant Support before 1.0.0.24 has unknown impact and remote attack vectors, a different vulnerability than CVE-2007-5608 and CVE-2008-0952.	unknown 2008-06-04	10.0	CVE-2008-0953 HP
HP -- storageworks_storage_mirroring	Stack-based buffer overflow in DoubleTake.exe in HP StorageWorks Storage Mirroring (SWSM) before 4.5 SP2 allows remote attackers to execute arbitrary code via a crafted encoded authentication request.	unknown 2008-06-04	10.0	CVE-2008-1661 XF
IBM -- AIX	Buffer overflow in the kernel in IBM AIX 5.2, 5.3, and 6.1 allows localusers to execute arbitrary code in kernel mode via unknown attack vectors.	unknown 2008-06-02	7.2	CVE-2008-2513 OTHER-REF AIXAPAR AIXAPAR AIXAPAR BID SECTRACK
IBM -- AIX	Unspecified vulnerability in iostat in IBM AIX 5.2, 5.3, and 6.1 allowslocal users to gain privileges via unknown vectors related to an"environment variable handling error."	unknown 2008-06-02	7.2	CVE-2008-2515 OTHER-REF AIXAPAR AIXAPAR AIXAPAR SECTRACK
icona -- instant_messenger	The DownloaderActiveX Control (DownloaderActiveX.ocx) in Icona SpA C6 Messenger 1.0.0.1 allows remote attackers to force	unknown 2008-06-04	9.3	CVE-2008-2551 BUGTRAQ MILW0RM

	the download and execution of arbitrary files via a URL in the propDownloadUrl parameter with the propPostDownloadAction parameter set to "run."			XF
Microsoft -- windows_installer	Stack-based buffer overflow in msiexec.exe 3.1.4000.1823 and 4.5.6001.22159 in Microsoft Windows Installer allows context-dependent attackers to execute arbitrary code via a long GUID value for the /x (aka /uninstall) option. NOTE: this issue might cross privilege boundaries if msiexec.exe is reachable via components such as ActiveX controls, and might additionally require a separate vulnerability in the control.	unknown 2008-06-04	9.3	CVE-2008-2547 BUGTRAQ BUGTRAQ BUGTRAQ OTHER-REF
Motorola -- razr	Stack-based buffer overflow in the JPEG thumbprint component in the EXIF parser on Motorola cell phones with RAZR firmware allows user-assisted remote attackers to execute arbitrary code via an MMS transmission of a malformed JPEG image, which triggers memory corruption.	unknown 2008-06-04	9.3	CVE-2008-2548
Pan -- Pan	The PartsBatch class in Pan 0.132 and earlier does not properly manage thedata structures for Parts batches, which allows remote attackers to cause adenial of service (application crash) and possibly execute arbitrary code via acrafted .nzb file that triggers a heap-based buffer overflow.	unknown 2008-06-02	9.3	CVE-2008-2363 OTHER-REF BID XF
quickupcms -- quickupcms	Multiple SQL injection vulnerabilities in Concepts & Solutions QuickUpCMS allow remote attackers to execute arbitrary SQL commands via the (1) nr parameter to (a) frontend/news.php, the (2) id parameter to (b) events3.php and (c) videos2.php in frontend/, the (3) y parameter to (d) frontend/events2.php, and the (4) ser parameter to (e) frontend/fotos2.php.	unknown 2008-06-03	7.5	CVE-2008-2530 MILW0RM BID XF
RakNet -- Autopatcher Server	SQL injection vulnerability in the Autopatcher server plugin in RakNet before 3.23 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	unknown 2008-06-03	7.5	CVE-2008-2523 OTHER-REF
Slashcode.com -- Slash	SQL injection vulnerability in Slashdot Like Automated Storytelling Homepage (Slash) (aka Slashcode) R_2_5_0_94 and earlier allows remote attackers to execute SQL commands and read table information via the id parameter.	unknown 2008-06-05	7.5	CVE-2008-2231 MLIST MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF
Sun -- java_active_server	The Admin Server in Sun Java Active Server Pages (ASP) Server before 4.0.3 allows remote attackers to append to arbitrary new or existing files via the first argument to a certain file that is included by multiple unspecified ASP applications.	unknown 2008-06-04	7.5	CVE-2008-2401 IDEFENSE SUNALERT
Sun -- Java ASP Server	Multiple directory traversal vulnerabilities in unspecified ASP applications in Sun Java Active Server Pages (ASP) Server before 4.0.3 allow remote attackers to read or delete arbitrary files via	unknown 2008-06-04	10.0	CVE-2008-2403 IDEFENSE

	a .. (dot dot) in the Path parameter to the MapPath method.			
Sun -- Java ASP Server	Stack-based buffer overflow in the request handling implementation in Sun Java Active Server Pages (ASP) Server before 4.0.3 allows remote attackers to execute arbitrary code via an unspecified string field.	unknown 2008-06-04	10.0	CVE-2008-2404 IDEFENSE
Sun -- java_active_server_pages	Sun Java Active Server Pages (ASP) Server before 4.0.3 allows remote attackers to execute arbitrary commands via shell metacharacters in HTTP requests to unspecified ASP applications.	unknown 2008-06-04	7.5	CVE-2008-2405 IDEFENSE SUNALERT
Sun -- Java ASP Server	The administration application server in Sun Java Active Server Pages (ASP) Server before 4.0.3 allows remote attackers to bypass authentication via direct requests on TCP port 5102.	unknown 2008-06-04	7.5	CVE-2008-2406 IDEFENSE SUNALERT
Sun -- Sun Cluster	The Sun Cluster Global File System in Sun Cluster 3.1 on Sun Solaris 8 through 10, when an underlying ufs filesystem is used, might allow local users to read data from arbitrary deleted files, or corrupt files in global filesystems, via unspecified vectors.	unknown 2008-06-03	7.2	CVE-2008-2539 SUNALERT BID XF
VMWare -- esxi VMWare -- VMware Server VMWare -- VMWare Workstation VMWare -- Player VMWare -- ESX Server	Untrusted search path vulnerability in vmware-authd in VMware Workstation 5.x before 5.5.7 build 91707 and 6.x before 6.0.4 build 93057, VMware Player 1.x before 1.0.7 build 91707 and 2.x before 2.0.4 build 93057, and VMware Server before 1.0.6 build 91891 on Linux, and VMware ESXi 3.5 and VMware ESX 2.5.4 through 3.5, allows local users to gain privileges via an unspecified option in a configuration file.	unknown 2008-06-05	7.2	CVE-2008-0967 IDEFENSE BUGTRAQ OTHER-REF SECTRACK
VMWare -- esxi VMWare -- ESX Server	The openwsman management service in VMware ESXi 3.5 and ESX 3.5 allows remote authenticated users to gain privileges via unspecified vectors related to "invalid Content-Length."	unknown 2008-06-05	9.0	CVE-2008-2097 BUGTRAQ OTHER-REF SECTRACK
VMWare -- Fusion VMWare -- esxi VMWare -- VMware Server VMWare -- ACE VMWare -- VMWare Workstation VMWare -- Player VMWare -- ESX Server	Multiple buffer overflows in VIX API 1.1.x before 1.1.4 build 93057 on VMware Workstation 5.x and 6.x, VMware Player 1.x and 2.x, VMware ACE 2.x, VMware Server 1.x, VMware Fusion 1.x, VMware ESXi 3.5, and VMware ESX 3.0.1 through 3.5 allow guest OS users to execute arbitrary code on the host OS via unspecified vectors.	unknown 2008-06-05	7.2	CVE-2008-2100 BUGTRAQ OTHER-REF SECTRACK
YABSoft -- Advanced Image Hosting Script	SQL injection vulnerability in out.php in YABSoft Advanced Image Hosting (AIH) Script 2.1 and earlier allows remote attackers to execute arbitrary SQL commands via the t parameter.	unknown 2008-06-03	7.5	CVE-2008-2536 MILW0RM BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
ActualScripts -- actualanalyzer_server ActualScripts -- actualanalyzer_gold ActualScripts -- actualanalyzer_pro ActualScripts -- actualanalyzer_lite	Cross-site scripting (XSS) vulnerability in view.php in ActualScripts ActualAnalyzer Server 8.37 and earlier, ActualAnalyzer Gold 7.74 and earlier, ActualAnalyzer Pro 6.95 and earlier, and ActualAnalyzer Lite 2.78 and earlier allows remote attackers to inject arbitrary web script or HTML via the language parameter.	unknown 2008-06-03	4.3	CVE-2008-2527 OTHER-REF BID
Adobe -- Acrobat Reader	Adobe Acrobat Reader 8.1.2 and earlier allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a malformed PDF document, as demonstrated by 2008-HI2.pdf.	unknown 2008-06-04	4.3	CVE-2008-2549 MILW0RM BID
Apache -- Tomcat	Cross-site scripting (XSS) vulnerability in Apache Tomcat 5.5.9 through 5.5.26 and 6.0.0 through 6.0.16 allows remote attackers to inject arbitrary web script or HTML via the name parameter (aka the hostname attribute) to host-manager/html/add.	unknown 2008-06-04	4.3	CVE-2008-1947 BUGTRAQ MLIST OTHER-REF OTHER-REF XF
Apple -- Mac OS X Server Apple -- Mac OS X	Apple Filing Protocol (AFP) Server in Apple Mac OS X before 10.5.3 doesnot verify that requested files and directories are inside shared folders, whichallows remote attackers to read arbitrary files via unspecified AFP traffic.	unknown 2008-06-02	6.8	CVE-2008-1027 APPLE CERT BID SECTRACK XF
Apple -- Mac OS X Server Apple -- Mac OS X	CoreGraphics in Apple Mac OS X before 10.5.3 allows remote attackers toexecute arbitrary code or cause a denial of service (application crash) via acrafted PDF document, related to an uninitialized variable.	unknown 2008-06-02	6.8	CVE-2008-1031 APPLE CERT BID SECTRACK XF
Apple -- Mac OS X Server Apple -- Mac OS X	Incomplete blacklist vulnerability in CoreTypes in Apple Mac OS X before10.5.3 allows user-assisted remote attackers to execute arbitrary code via an(1) Automator, (2) Help, (3) Safari, or (4) Terminal content type for adownloadable object, which does not trigger a "potentially unsafe"warning message in (a) the Download Validation feature in Mac OS X 10.4 or (b)the Quarantine feature in Mac OS X 10.5.	unknown 2008-06-02	6.8	CVE-2008-1032 SECTRACK XF
Apple -- Mac OS X Server Apple -- Mac OS X	The scheduler in CUPS in Apple Mac OS X 10.5 before 10.5.3, when debuglogging is enabled and a printer requires a password, allows attackers to obtainsensitive information (credentials) by reading the log data, related to"authentication environment variables."	unknown 2008-06-02	6.0	CVE-2008-1033 APPLE CERT BID SECTRACK XF
Apple -- Mac OS X Server Apple -- Mac OS X	Integer underflow in Help Viewer in Apple Mac OS X before 10.5 allowsremote attackers to execute arbitrary code or cause a denial of service(application crash) via a crafted help:topic URL that triggers a bufferoverflow.	unknown 2008-06-02	6.8	CVE-2008-1034 APPLE CERT CERT-VN BID SECTRACK XF

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Discovered Published**	**CVSS Score**	**Source & Patch Info**
Apple -- Mac OS X Server Apple -- Mac OS X	The sso_util program in Single Sign-On in Apple Mac OS X before 10.5.3places passwords on the command line, which allows local users to obtainsensitive information by listing the process.	unknown 2008-06-02	2.1	CVE-2008-1578 BID SECTRACK XF
libpam-pgsql -- libpam-pgsql	pam_sm_authenticate in pam_pgsql.c in libpam-pgsql 0.6.3 does not properly consider operator precedence when evaluating the success of a pam_get_pass function call, which allows local users to gain privileges via a SIGINT signal when this function is executing, as demonstrated by a CTRL-C sequence at a sudo password prompt in an "auth sufficient pam_pgsql.so" configuration.	unknown 2008-06-03	2.1	CVE-2008-2516 OTHER-REF BID SECTRACK
SourceForge -- SaraB	The sarab.sh script in SaraB before 0.2.4 places the dar program's encryption key on the command line, which allows local users to obtain sensitive information by listing the process.	unknown 2008-06-03	2.1	CVE-2008-2517 OTHER-REF OTHER-REF OTHER-REF BID XF

Back to top